УДК 004.056.55; 004.056.53;
УДК 004.056.52

Д.В. Фомин

МОДИФИКАЦИЯ МЕТОДА СКРЫТИЯ ИНФОРМАЦИИ КУТТЕРА – ДЖОРДАНА – БОССЕНА

В статье предлагается модификация метода Куттера – Джордана – Боссена, применяющегося в стеганографии для скрытия информации в пространственной области растрового изображения. Данная модификация позволяет уменьшить изменения, вносимые в контейнер при встраивании сообщения, что повышает надежность метода.

Ключевые слова: стеганография, скрытие данных, информационная безопасность, защита информации, внедрение данных, оценка метода.

MODIFICATION OF THE KUTTER – JORDAN – BOSSEN METHOD OF INFORMATION HIDING

This article contains description of the Kutter – Jordan – Bossen method of information hiding in a spatial area of a bitmap image and modification of this method. Modification allows to reduce container changing through information embedding what improves stegodetect protection.

Key words: steganography, data hiding, information security, data protection, implementation data, assessment method.

Задача защиты информации от несанкционированного доступа, изменения, уничтожения существует уже давно. В ходе поиска решения сформировались два основных подхода, а затем и две соответствующие науки: криптография и стеганография. Криптография защищает содержимое сообщения – например, шифруя его, а стеганография скрывает сам факт существования секретного сообщения. Нередко методы обеих наук применяются совместно, – к примеру: сообщение может быть зашифровано, а потом скрыто, таким образом повышается стойкость передаваемого сообщения.

В рамках стеганографии существуют три направления: классическая, компьютерная и цифровая стеганография. Цифровая стеганография основывается на внедрении информации в цифровые объекты, вызывая некоторые искажения объектов. Это направление стеганографии нашло свое применение в решении следующих задач: скрытый обмен информацией, защита авторских прав (встраивание ЦВЗ и «отпечатков пальцев»), хранение информации, не предусмотренной форматом цифрового объекта-контейнера (встраивание заголовков) [3].

Цифровая стеганография использует избыточность цифрового контейнера для внедрения в него скрытого сообщения, при этом изменения, возникающие в контейнере, не должны быть заметны ни органам чувств среднестатистического человека, ни специальным программным и аппаратным средствам. Изменения не должны нарушать функциональность контейнера. Кроме того, объем стего-контейнера должен быть достаточным для встраивания сообщения необходимого объема.

Наиболее подходящими контейнерами фиксированной длины [1] являются мультимедиа файлы: они имеют достаточно большой объем и избыточность, широко распространены и не вызывают

подозрений. Существует ряд методов для встраивания сообщений в контейнеры данных типов. Большинство из методов, работающих с каким-либо конкретным типом контейнера, после адаптации применимо и к другим типам.

Среди стеганографических методов, применяемых к файлам-изображениям, стоит обратить внимание на метод Куттера – Джордана – Боссена. Он обладает высокой пропускной способностью, устойчивостью к искажениям, устойчивостью к основным видам атак [2]. Благодаря своим характеристикам данный метод позволяет передавать сообщение в файлах формата JPEG и устойчив к разрушению младших бит контейнера, что невозможно для более известного метода наименьших значащих бит.

Но у метода Куттера – Джордана – Боссена есть недостатки. Один из них – вероятностное извлечение сообщения. То есть сообщение, встроенное в контейнер отправителем, может быть верно восстановлено из стего адресатом только с некоторой высокой вероятностью. Кроме того, существует несколько проблем, становящихся заметными при реализации и практическом применении данного метода. Решения этих проблем предложены в [4].

Для увеличения вероятности безошибочного восстановления сообщения авторы метода предлагают встраивать секретное сообщение более одного раза в один и тот же контейнер [2]. Но с повышением вероятности успешного восстановления таким способом возрастает и заметность изменений, вносимых в контейнер при встраивании, так как увеличиваются изменения в контейнере по сравнению с его исходным состоянием. Для уменьшения изменений, вносимых в контейнер при встраивании сообщения, предлагается модифицировать алгоритм встраивания сообщения.

Метод Куттера – Джордана – Боссена основывается на том, что зрение среднестатистического человека наименее чувствительно к синему цвету [2]. Соответственно, метод предлагает встраивание сообщения в синий канал изображения-контейнера в цветовой модели RGB [4].

Встраивание сообщения данным методом реализуется следующим образом. M – массив бит сообщения: m_i – i-й бит сообщения; $C\{R,G,B\}$ – изображение-контейнер; $p(x,y)$ – пиксель контейнера, в который будет производиться встраивание.

Бит сообщения встраивается в канал синего цвета путем модификации яркости выбранного пикселя. Для этого определяется яркость пикселя контейнера:

$$\lambda_{x,y}=0{,}29890\cdot R_{x,y}+0{,}58662\cdot G_{x,y}+0{,}11448\cdot B_{x,y},$$

где $\lambda_{x,y}$ – яркость пикселя, а $R_{x,y}$, $G_{x,y}$, $B_{x,y}$ – значения соответствующих коэффициентов пикселя контейнера.

Затем модифицируется значение $B_{x,y}$:

$$B'_{x,y}=\begin{cases}B_{x,y}-\upsilon\cdot\lambda_{x,y}, \text{ при } m_i=0;\\ B_{x,y}+\upsilon\cdot\lambda_{x,y}, \text{ при } m_i=1.\end{cases}=B_{x,y}+(2\cdot m_i-1)\cdot\upsilon\cdot\lambda_{x,y},$$

где v – константа, определяющая энергию встраиваемого сигнала. Чем больше v, тем сообщение устойчивее к искажениям, но, вместе с тем заметнее [2].

Извлечение сообщения не требует исходного контейнера и происходит следующим образом. Выбирается пиксель контейнера, в который был встроен бит сообщения. Затем производится оценка интенсивности синей цветовой составляющей данного пикселя на основе соседних пикселей. В [2] для оценки предлагается использовать «крест пикселей 7x7», при этом в центре «креста» должен находиться оцениваемый пиксель.

$$B^{\text{прог}}_{x,y}=\frac{1}{4\sigma}\left(\sum_{i=-\sigma}^{+\sigma}B_{x+i,y}+\sum_{j=-\sigma}^{+\sigma}B_{x,y+j}-2\cdot B_{x,y}\right)$$

где $B^{\text{прог}}_{x,y}$ – прогнозируемое значение синей цветовой составляющей, а σ – количество пикселей в стороны по вертикали и горизонтали от оцениваемого. В случае креста 7x7, $\sigma = 3$.

Далее рассчитывается разница δ между полученным оценочным значением и реальным:

$\delta = B_{x,y} - B_{x,y}^{\text{прог}}$.

Если $\delta < 0$, то $m = 0$; если $\delta > 0$, то $m = 1$.

Достоинствами метода Куттера – Джордана – Боссена являются:

1) высокая пропускная способность;

2) высокая устойчивость к несанкционированному ознакомлению;

3) высокая устойчивость к частотному детектированию;

4) высокая устойчивость к разрушению младших бит контейнера;

5) устойчивость к обрезанию краев;

6) устойчивость к атаке сжатия.

Таким образом, данный метод позволяет скрывать информацию не только в файлах формата BMP, но и в JPEG-контейнерах: для встраивания нужно растравое представление изображения (BMP), но после встраивания изображение можно конвертирвоать в формат JPEG. Благодаря устойчивости к сжатию встроенное сообщение при этом сохранится, а контейнер будет меньше привлекать внимания, так как формат JPEG на данный момент более распространен.

Для оценки качества стеганографических методов авторы [5] предлагают использовать следующие показатели:

1. Соотношение «сигнал/шум»

$$SNR = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left(C_{x,y}\right)^2}{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left(C_{x,y} - S_{x,y}\right)^2},$$

где $C_{x,y}$ – значение пикселя пустого контейнера с координатами (x, y); $S_{x,y}$ – соответствующее значение пикселя заполненного контейнера; $rows\ (C)$ – количество строк в массиве C; $cols\ (C)$ – количество столбцов в массиве C.

2. Нормированная средняя абсолютная разница, указывающая степень отличия между пустым контейнером и стегоконтейнером

$$NAD = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left|C_{x,y} - S_{x,y}\right|}{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left|C_{x,y}\right|},$$

3. Качество изображения, характеризующее степень визуальных различий между контейнером и стего

$$IF = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left(C_{x,y} - S_{x,y}\right)^2}{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left(C_{x,y}\right)^2},$$

4. Структурное содержание, также характеризующее величину искажений, вносимых в контейнер

$$SNR = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left(C_{x,y}\right)^2}{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left(S_{x,y}\right)^2}.$$

Описанная модификация предлагает заменить безусловное изменение параметров пикселя контейнера на замену с проверкой условия. То есть надо перед расчетом нового значения $B_{x,y}$ пикселя контейнера найти разность между его оценкой и текущим значением, а затем «сэмулировать» извлечение бита сообщения, просто сравнив значение полученной разности δ с 0. Тогда, если результат сравнения соответствует значению встраиваемого бита, можно считать, что бит уже встроен и может быть восстановлен при извлечении сообщения. Остается сравнить величину δ с минимальным значением, определяемым выбранной энергией встраиваемого сигнала. Если δ окажется недостаточной,

значение $B_{x,y}$ пикселя необходимо изменить, но лишь на недостающую величину, а значит, изменения будут меньше, чем без предлагаемой проверки.

Таким образом, алгоритм встраивания примет вид (без модификаций, предложенных в [4]):

1) взять бит сообщения m_i;

2) выбрать пиксель контейнера $p(x,y)$;

3) произвести сравнение значения синей цветовой составляющей пикселя $B_{x,y}$ с прогнозируемым $B_{x,y}^{\text{прог}}$;

4) если из текущего пикселя $p(x,y)$ извлекается бит, не соответствующий встраиваемому, то использовать стандартную формулу встраивания:

$$B'_{x,y} = \begin{cases} B_{x,y} - \upsilon \cdot \lambda_{x,y}, \text{ при } m_i = 0 \\ B_{x,y} + \upsilon \cdot \lambda_{x,y}, \text{ при } m_i = 1 \end{cases} = B_{x,y} + (2 \cdot m_i - 1) \cdot \upsilon \cdot \lambda_{x,y};$$

5) если выполняются следующие условия: $\left|B_{x,y} - B_{x,y}^{\text{прог}}\right| \geq \upsilon \cdot \lambda_{x,y}$ (энергия встроенного сигнала не меньше необходимой); $\left(B_{x,y} - B_{x,y}^{\text{прог}}\right) > 0$, при $m_i = 1$ и, при $m_i = 0$ (читается верное значения бита сообщения), то пиксель $p(x,y)$ содержит бит секретного сообщения m_i с энергией, не меньшей заданной;

6) если не выполняется условие, накладываемое на энергию сигнала, т.е. $\left|B_{x,y} - B_{x,y}^{\text{прог}}\right| < \upsilon \cdot \lambda_{x,y}$, но читается верное значение бита, то применяем стандартную формулу встраивания, в которой вместо $\upsilon \cdot \lambda_{x,y}$ используем $\Delta = \upsilon \cdot \lambda_{x,y} - \left|B_{x,y} - B_{x,y}^{\text{прог}}\right|$, таким образом добавляем недостающую энергию.

Произведем оценку модифицированного метода по приведенным в [4] методикам:

1. Соотношение «сигнал/шум»

$$SNR = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left(C_{x,y}\right)^2}{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left(C_{x,y} - S_{x,y}\right)^2}$$

Так как мы уменьшаем вносимые изменения в пиксели контейнера, то

$S_{x,y} \to C_{x,y} \Rightarrow \left(C_{x,y} - S_{x,y}\right) \to 0 \Rightarrow SNR \to 1$, $SNR_{станд.} < SNR_{мод.} < 1$.

2. Нормированная средняя абсолютная разница

$$NAD = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left|C_{x,y} - S_{x,y}\right|}{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left|C_{x,y}\right|},$$

Так как модификация уменьшает вносимые изменения в пиксели контейнера, то

$S_{x,y} \to C_{x,y} \Rightarrow \left|C_{x,y} - S_{x,y}\right| \to 0 \Rightarrow NAD \to 0$, $NAD_{станд.} > NAD_{мод.} > 0$.

3. Качество изображения

$$IF = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left(C_{x,y} - S_{x,y}\right)^2}{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left(C_{x,y}\right)^2}$$

Так как модификация уменьшает вносимые изменения в пиксели контейнера, то

$S_{x,y} \to C_{x,y} \Rightarrow \left(C_{x,y} - S_{x,y}\right) \to 0 \Rightarrow IF \to 0$, $IF_{станд.} > IF_{мод.} > 0$.

4. Структурное содержание

$$SC = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left(C_{x,y}\right)^2}{\sum_{x=1}^{row(C)} \sum_{y=1}^{col(C)} \left(S_{x,y}\right)^2}$$

Так как модификация уменьшает вносимые изменения в пиксели контейнера, то

$$S_{x,y} \to C_{x,y} \Rightarrow \frac{C_{x,y}}{S_{x,y}} \to 1 \Rightarrow SC \to 1,\ SC_{станд.} < SC_{мод.} < 1.$$

Таким образом, предложенная модификация дает улучшение вышеперечисленных показателей и сохраняет энергию встраиваемого сигнала, а значит, – и устойчивость к искажениям. Но при этом несколько усложняется алгоритм встраивания.

Данная модификация позволяет уменьшить изменения, вносимые в контейнер, что повысит скрытность передачи сообщения, если пикселей, к которым применима предлагаемая модификация, в сообщении достаточное количество. Иначе эффект от изменения метода будет слишком мал.

У метода Куттера – Джордана – Боссена отмечается ряд недостатков, в том числе вероятностное извлечение скрытого сообщения. Для повышения вероятности безошибочного извлечения авторы метода предлагают кратное встраивание сообщения в один и тот же контейнер, что дает желаемый результат, но увеличивает заметность встроенного сообщения. Предложенная модификация метода предлагает изменить алгоритм встраивания отдельного бита сообщения таким образом, чтобы учитывалась возможность нахождения данного бита сообщения в данном пикселе контейнера. Применение такой модификации позволяет уменьшить изменения, вносимые в контейнер. Но эффективность предложенной модификации предстоит оценить экспериментально.

1. Генне, О.В. Основные положения стеганографии // Защита информации. – 2000. – № 3.

2. Коханович, Г.Ф., Пузыренко, А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.

3. Грибунин, В.Г., Оков, И.Н., Туринцев, И.В. Цифровая стеганография. – М.: СОЛОН-ПРЕСС, 2009. – 277 с.

4. Защелкин, К.В., Иващенко, А.И., Иванова, Е.Н. Усовершенствование метода скрытия данных Куттера – Джордана – Боссена // МНПК «Современные информационные и электронные технологии», 2013.

5. Вовк, О.О., Астраханцев, А.А., Дорожан, А.В. Исследование стойкости методов скрытия информации в неподвижных изображениях // Радіоелектронні і комп’ютерні системи. – 2012. – № 2.